



QUALYS SECURITY CONFERENCE 2019

DevOps at Qualys

DevOps Transformation of the Qualys Platform: Lessons Learned

Dilip Bachwani

SVP, Engineering and Cloud Operations, Qualys, Inc.

Massive Expansion of Cloud Platform

19+ products and counting

95+ cloud platform deployments

150+ microservices on containers

High-volume big data clusters

Platform volumes and Infrastructure doubled over past year

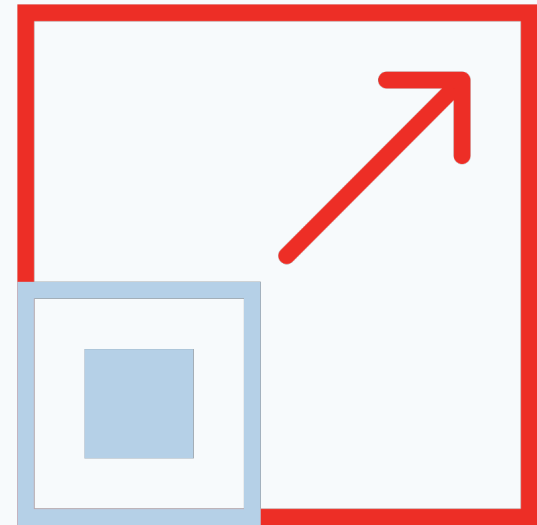
Engineering teams have grown multifold



Growing Pains...

Keep up the release velocity... but not lose operational stability and reliability

However, 19+ products deployed across 95+ platforms can introduce significant operational complexity



DevOps

Infra & Ops as a software problem

Dev and Ops sharing ownership in production

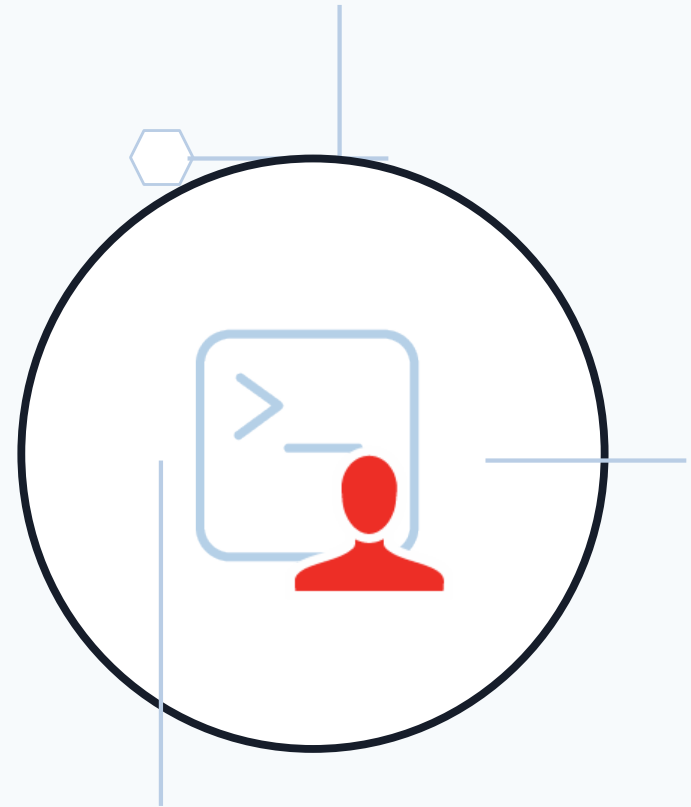
Fully automated one-click deployments

Configuration management driven by code

Robust logging, monitoring and alerting

Security *must* be built-in

Address silos – people, process and tools

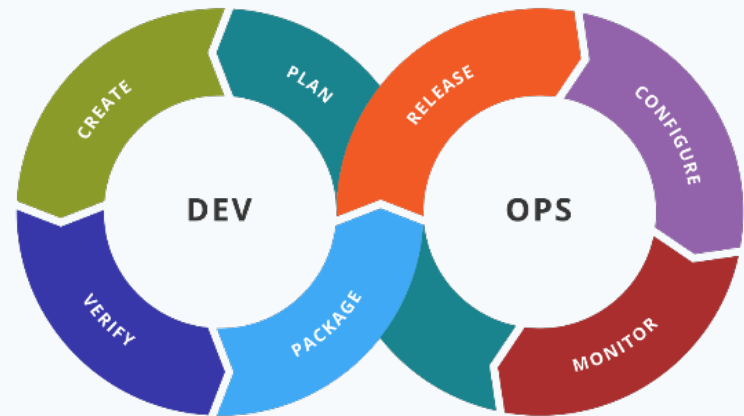


Robust DevOps Toolchain

Combine and orchestrate effective set of tools for developing, delivering and maintaining software

Standardized toolchain on a common platform available to everyone

Hub and spoke DevOps model



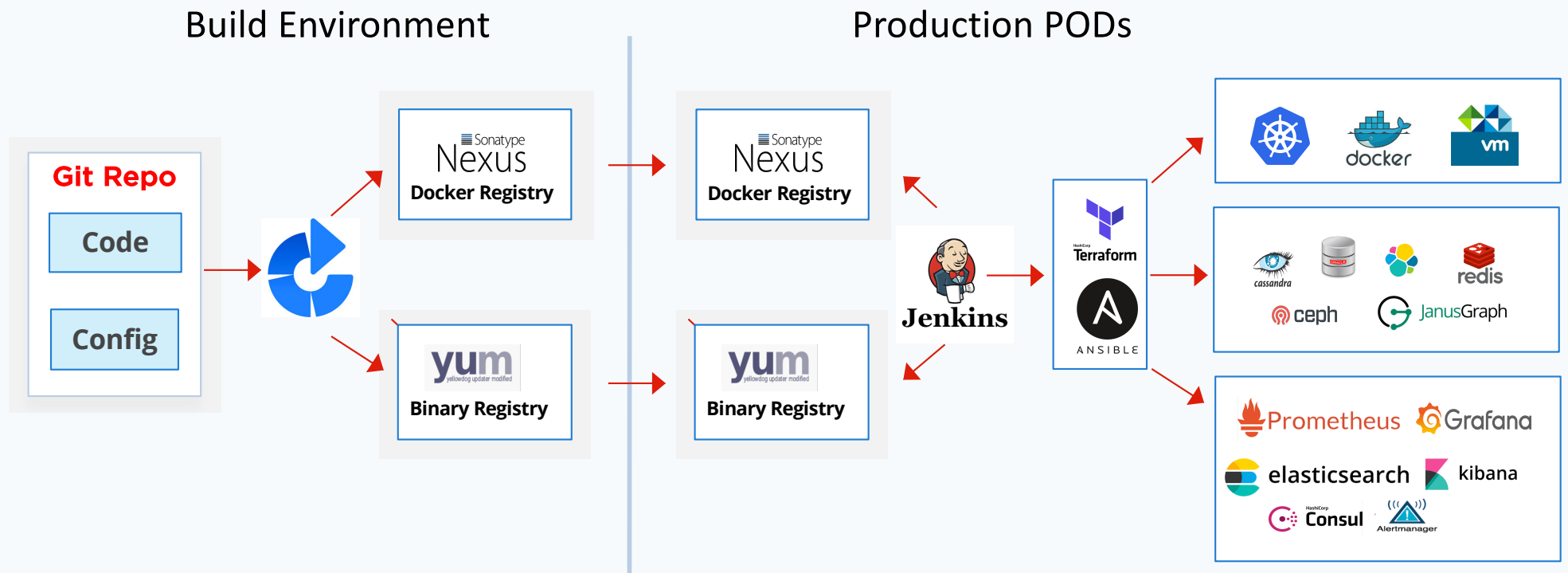
One-click No-touch Deployments

Fully automated build, release and deployment pipelines

End-to-end configuration management across everything



One-click No-touch Deployments



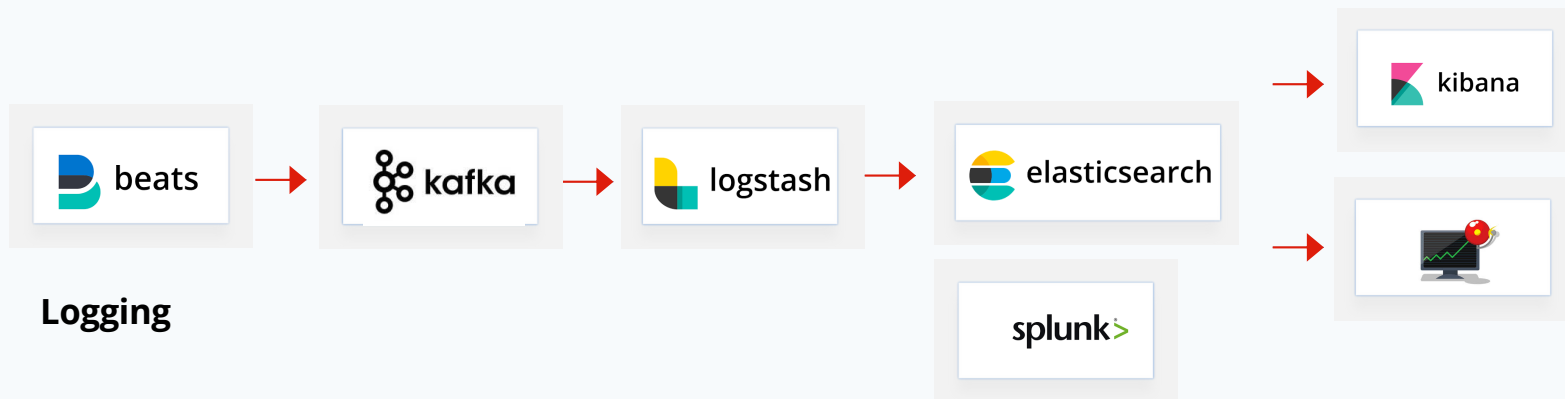
Observability

Comprehensive infrastructure,
network and application monitoring

Aggregate data across all platforms
into a single-pane view



Logging, Monitoring & Alerting



Monitoring



Other



Site Reliability Engineering

Engineers running systems in production

Product teams with SREs own how they build, release, deploy, configure and monitor their own products and services

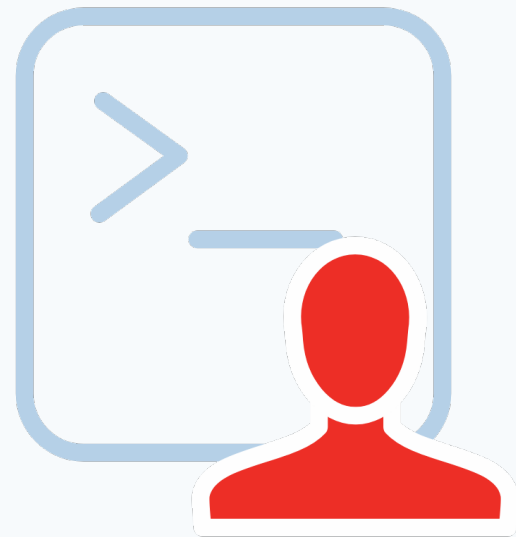


Build Security into CI/CD Pipeline

Standardized DevOps process and toolchain enables built-in security

Static code analysis, vulnerability, compliance, image & WAS scans integrated into CI/CD pipeline

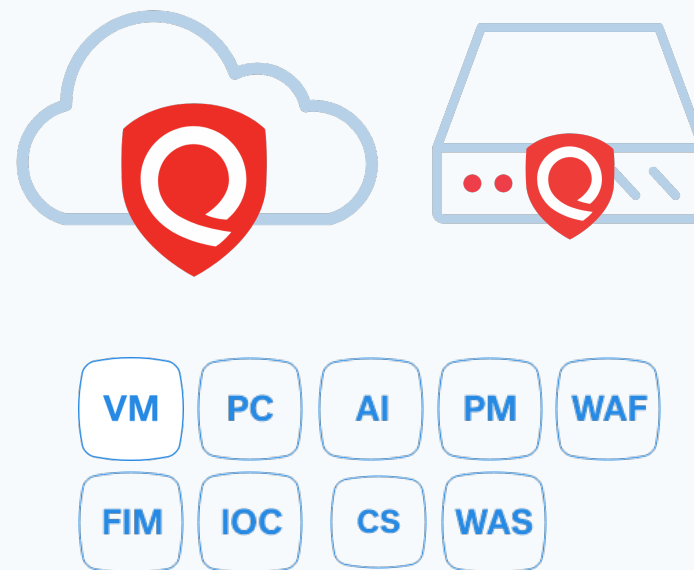
Automated patching



Qualys-on-Qualys

Infrastructure-as-code bakes in Qualys Cloud Agent into every host

Understand vulnerability and threat exposure in real-time



HIGH - STATUS < 30 DAYS

VULNERABILITY STATUS COUNT

ACTIVE 499

FIXED 399

NEW 20

REOPENED 7

HIGH - 1ST-FOUND < 30 DAYS

526

showing last 91 days ⚙



HIGH-FOUND&PUBLISHED<30DA...

77

showing last 91 days ⚙



HIGH - PUBLISHED < 30 DAYS

VULNERABILITY STATUS COUNT

ACTIVE 73

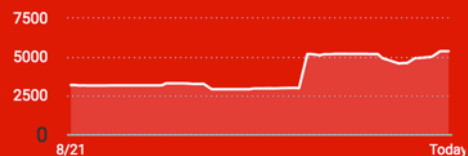
FIXED 30

NEW 4

HIGH-1-ST-FOUND > 30 DAYS

5.37K

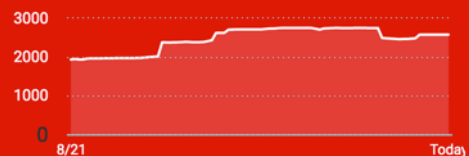
showing last 91 days ⚙



HIGH-1-ST-FOUND > 90 DAYS

2.58K

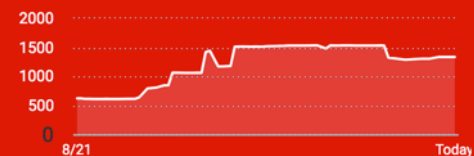
showing last 91 days ⚙



HIGH-1-ST-FOUND > 180 DAYS

1.33K

showing last 91 days ⚙



TOP 50 - MEDIUM VULNERABILITIES

VULNERABILITY TITLE

COUNT

SSL/TLS Server supports TLSv1.0

15

Birthday attacks against TLS ciphers with 64bit block size vulnerability (Sweet32)

13

TCP Sequence Number Approximation Based Denial of Service

11

UDP Constant IP Identification Field Fingerprinting Vulnerability

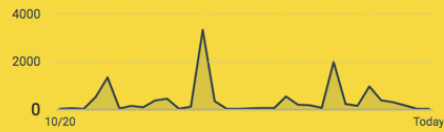
10



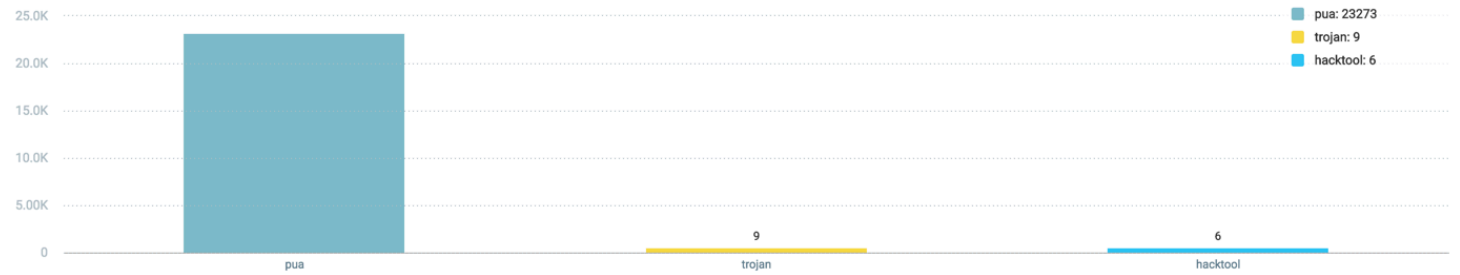
THREAT FEED 7 - 10

11.7K

showing last 30 days ⚙️



MALWARE CATEGORY



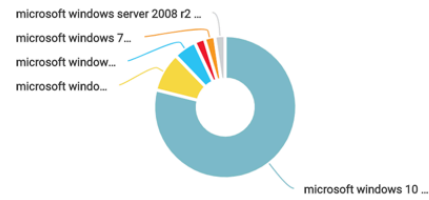
IOC - SEVERITY 6 - 10

NAME	COUNT
proxgater	11385
proxgate	148
webcompanion	117
lobit	4
control	2
corebot	2
trickbot	2

DUAL USE TOOL: REMOTE ADMIN UTILITY

NAME	COUNT
c:\program files (x86)\teamviewer	24
c:\program files\teamviewer	4

TOP OS INFECTED



TROJAN: PASSWORD DUMPING TOOLS

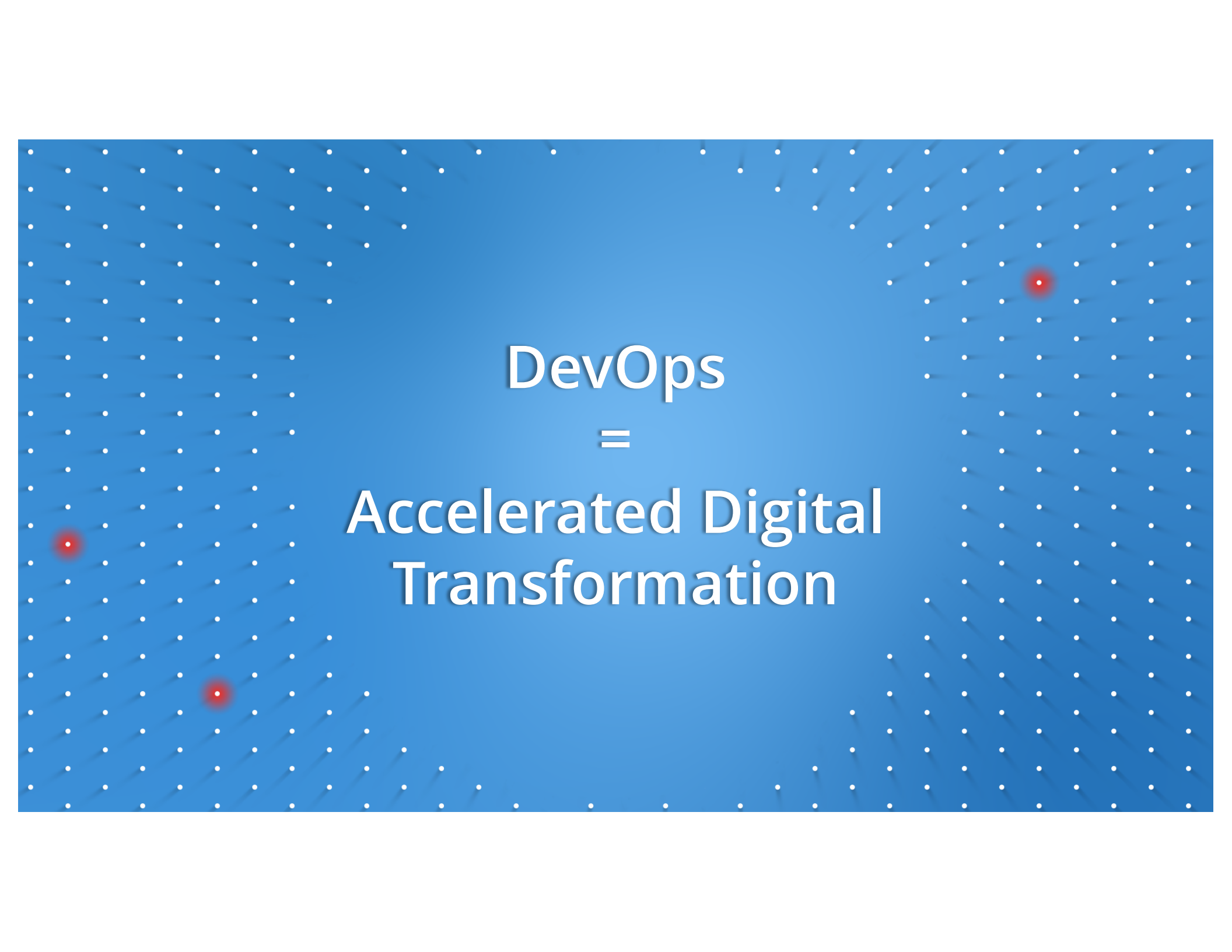
No data available

REMOTE IPS | SCORE: 7 - 10

NAME	COUNT
67.229.60.114	1126
174.139.78.106	952

THREAT SCORE < 5

NAME	COUNT
878d28d5007ef609e812f08c580b0142032deac545bcb673a37830aec0d7d430	138
8e5b13e4ddeb1b2e3e63327624a91dda2ae7c735da73b015c08550fb85b82424	5



DevOps
=
Accelerated Digital
Transformation



QUALYS SECURITY CONFERENCE 2019

Dilip Bachwani
dbachwani@qualys.com